

**WHAT IS CLAIMED IS:**

- 1 1. A method for analyzing database security, said method  
2 comprising:  
3 connecting to one or more servers, wherein each server  
4 includes an instance, the instance including one  
5 or more databases;  
6 selecting one of the databases;  
7 identifying a user id, wherein the user id has access  
8 to the selected databases;  
9 retrieving a permitted user id list corresponding to  
10 the selected database;  
11 determining whether the user id is included in the  
12 permitted user id list;  
13 reporting the user id in response to the determining.
- 1 2. The method as described in claim 1 further comprising:  
2 retrieving a resolution corresponding to the  
3 determining; and  
4 including the resolution in the reporting.
- 1 3. The method as described in claim 1 wherein the  
2 determining further comprises:  
3 identifying a violation message type wherein the  
4 violation message type is selected from the group  
5 consisting of a removed users check, a DB files  
6 and logs access check, and a DB backup files and  
7 logs access check.
- 1 4. The method as described in claim 1 wherein the  
2 database is selected from a group consisting of a  
3 database, a backup database, and a directory of  
4 databases.

- 1 5. The method as described in claim 1 wherein the  
2 connection is secure.
- 1 6. The method as described in claim 1 wherein the  
2 permitted user id list is selected from the group  
3 consisting of a database instance owner, a sysadm  
4 group, and a sysmaint group.
- 1 7. The method as described in claim 1 wherein the servers  
2 are on different operating platforms.
- 3 8. An information handling system comprising:  
4 one or more processors;  
5 a memory accessible by the processors;  
6 one or more nonvolatile storage devices accessible by  
7 the processors;  
8 a database analysis tool to analyze database security,  
9 the database analysis tool including:  
10 means for connecting to one or more servers,  
11 wherein each server includes an instance,  
12 the instance including one or more  
13 databases;  
14 means for selecting one of the databases;  
15 means for identifying a user id, wherein the user  
16 id has access to the selected databases;  
17 means for retrieving a permitted user id list  
18 corresponding to the selected database;  
19 means for determining whether the user id is  
20 included in the permitted user id list;  
21 means for reporting the user id in response to  
22 the determining.

- 1 9. The information handling system as described in claim  
2 8 further comprising:  
3 retrieving a resolution corresponding to the  
4 determining; and  
5 including the resolution in the reporting.
- 1 10. The information handling system as described in claim  
2 8 wherein the determining further comprises:  
3 identifying a violation message type wherein the  
4 violation message type is selected from the group  
5 consisting of a removed users check, a DB files  
6 and logs access check, and a DB backup files and  
7 logs access check.
- 1 11. The information handling system as described in claim  
2 8 wherein the database is selected from a group  
3 consisting of a database, a backup database, and a  
4 directory of databases.
- 1 12. The information handling system as described in claim  
2 8 wherein the permitted user id list is selected from  
3 the group consisting of a database instance owner, a  
4 sysadm group, and a sysmaint group.
- 1 13. The information handling system as described in claim  
2 8 wherein the servers are on different operating  
3 platforms.
- 1 14. A computer program product stored in a computer  
2 operable media for analyzing database security, said  
3 computer program product comprising:

4 means for connecting to one or more servers, wherein  
5 each server includes an instance, the instance  
6 including one or more databases;  
7 means for selecting one of the databases;  
8 means for identifying a user id, wherein the user id  
9 has access to the selected databases;  
10 means for retrieving a permitted user id list  
11 corresponding to the selected database;  
12 means for determining whether the user id is included  
13 in the permitted user id list;  
14 means for reporting the user id in response to the  
15 determining.

1 15. The computer program product as described in claim 14  
2 further comprising:  
3 retrieving a resolution corresponding to the  
4 determining; and  
5 including the resolution in the reporting.

1 16. The computer program product as described in claim 14  
2 wherein the determining further comprises:  
3 identifying a violation message type wherein the  
4 violation message type is selected from the group  
5 consisting of a removed users check, a DB files  
6 and logs access check, and a DB backup files and  
7 logs access check.

1 17. The computer program product as described in claim 14  
2 wherein the database is selected from a group  
3 consisting of a database, a backup database, and a  
4 directory of databases.

1 18. The computer program product as described in claim 14  
2 wherein the connection is secure.

1 19. The computer program product as described in claim 14  
2 wherein the permitted user id list is selected from  
3 the group consisting of a database instance owner, a  
4 sysadm group, and a sysmaint group.

1 20. The computer program product as described in claim 14  
2 wherein the servers are on different operating  
3 platforms.

1004594 424704